



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/760,521

01/21/2004

Gabor Bajko

59643.00350

1094

32294 7590 11/23/2007  
SQUIRE, SANDERS & DEMPSEY L.L.P.  
14TH FLOOR  
8000 TOWERS CRESCENT  
TYSONS CORNER, VA 22182

EXAMINER

TURCHEN, JAMES R

ART UNIT

PAPER NUMBER

2139

MAIL DATE

DELIVERY MODE

11/23/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

**Office Action Summary**

Application No.

10/760,521

Applicant(s)

BAJKO ET AL.

Examiner

James Turchen

Art Unit

2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 14 September 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☒ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

Claims 1-28 are pending. Claims 1, 5, 7-13, 15, 16, 19-21, 24, and 25 are amended.

Claims 26-28 are new.

#### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 11 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

#### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over 3GPP TS 33.102 v5.1.0 (herein 3G Security) in view of Bacchus et al. hereafter Bacchus (US 7,219,223) and UMTS Security.

Regarding claim 1:

3G Security discloses a method in a communication system wherein a serving controller is configured to support a first security mechanism and at least one other security mechanism, the method comprising:

sending a request for registration from a user equipment to a serving controller via a second controller, said request for registration including information indicative of at least one security mechanism supported by the user equipment [*page 29 step 2 of figure 14, the MS (mobile station) transfers to VLR/SGSN the initial L3 message*];

determining based on the information in the second controller that the user equipment supports a second security mechanism other than a first security mechanism [*page 29 step 1 of figure 14, the MS transferred the START values and user equipment security capabilities; page 29 step 6 of figure 14, the SRNC decides which algorithm to use out of the user equipment security capabilities*];

including in the request for registration an indication that the second security mechanism is used by the user equipment [*page 30 step 11 of figure 14, SRNC sends VLR/SGSN Security Mode Complete response, including the selected algorithms*]; and

sending a challenge in accordance with the second security mechanism from the serving controller to the user equipment [*page 28 last paragraph, figure 14 (steps 1-11) are at initial connection establishment, possible authentication, and start of integrity protection and possible ciphering; page 20 figure 7 shows the generation of the cipher key (CK) and integrity key (IK) using f3 (UEA) and f4 (UIA) respectively; page 21 figure 8, discloses VLR/SGSN performing and authentication challenge (AUTN) with the USIM (on the user equipment)*].

3G Security does not disclose removing the information from the request for registration in the second controller. Bacchus is analogous to 3G security in that they both specify a proxy to select the cipher algorithms from a list. Bacchus discloses a

proxy method and system wherein the client transmits the cipher suite list to the proxy [column 9 lines 25-26] and the request is forwarded to the server along with the selected cipher [column 10 lines 16-22; *it is obvious that the other ciphers from the list are not sent, therefore they are removed*]. One of ordinary skill in the art at the time of invention could have combined the method of Bacchus with the method of 3G Security in order to forward only the selected cipher to the server [column 10 lines 16-22].

3G Security and Bacchus fail to disclose the use of a registration request. UMTS security is analogous to 3G Security as it relates to third generation cellular systems. UMTS Security discloses an IP multimedia subsystem using SIP [page 199 Section 5-page 200]. SIP uses registration requests from the user equipment to the serving controller [page 202 Figure 7]. It would have been obvious to one of ordinary skill in the art at the time of invention to add SIP as disclosed in UMTS Security in order to allow for a IP multimedia subsystem [page 199 Section 5-page 200].

Regarding claim 2:

3G Security discloses a method as claimed in claim 1, further comprising: including a response to the challenge in a message from the user equipment to the serving controller (page 23 first and second paragraphs, user equipment sends RES (response) to the challenge to VLR/SGSN).

Regarding claim 3:

3G security discloses a method as claimed in claim 2, further comprising: using the response for authentication of the message at the serving controller (page 23

second paragraph, if expected response is equal to response, then the authentication of the user has passed).

Regarding claim 4:

3G Security discloses a method as claimed in claim 1, further comprising: providing the second controller comprising a network entity providing proxy (page 29 VLR/SGSN performs security functions and access control). 3G Security does not disclose the second controller comprising a proxy call session control function. UMTS security discloses in figure 7 on page 202 a P-CSCF (corresponding to the VLR/SGSN of 3G Security).

It would have been obvious to one of ordinary skill in the art to modify the method of 3G Security to incorporate IMS of UMTS Security in order to deliver IP multimedia services to end users.

Regarding claim 5:

3G Security discloses a method as claimed in claim 1, wherein the step of sending the request for registration from the user equipment to the serving controller comprises sending a challenge from the serving controller to the user equipment (page 21 figure 8, discloses VLR/SGSN performing and authentication challenge (AUTN) with the USIM (on the user equipment)), sending a response to the challenge from the user equipment (page 23 first and second paragraphs, user equipment sends RES (response) to the challenge to VLR/SGSN), and registering the user equipment to the serving controller only if a satisfactory response is received from the user equipment (page 23 second paragraph, if expected response

is equal to response, then the authentication of the user has passed), and sending a further challenge to the user equipment after the registration step is completed (page 30, the nonce FRESH is sent from the VLR/SGSN to the UE; page 34, FRESH is a network side nonce; it is inherent that the nonce is used as a means of authenticating the MS in order to prevent replay attacks).

Regarding claim 6:

3G Security discloses a method as claimed in claim 1, further comprising: obtaining data for sending the challenge from a user information database (page 41 second paragraph, authentication challenge is retrieved from a local database).

Regarding claim 7:

3G Security discloses a method as claimed in claim 1, wherein the step of sending the challenge comprises sending the challenge comprising an authentication vector (figure 5 on page 18, shows the challenge comprising an authentication vector).

Regarding claim 8:

3G Security discloses a method as claimed in claim 1, but does not disclose providing the first security mechanism comprising a security mechanism in accordance with a Secure Internet Protocol. UMTS security discloses using IPsec (page 203, integrity protection using IPsec ESP). It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of 3G Security to include IPsec as disclosed in UMTS security in order to make messages integrity protected (page 203, Integrity protection using IPsec ESP).

Regarding claim 9:

3G Security discloses a method as claimed in claim 1, but does not disclose providing the second security mechanism comprising a security mechanism in accordance with a Hypertext Transfer Digest protocol. UMTS security discloses using HTTP Digest (page 202, Authentication using HTTP Digest AKA). It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of 3G Security to include HTTP Digest as disclosed in UMTS security in order to provide secure authentication (pages 202-203, Authentication using HTTP Digest AKA).

Regarding claim 10:

3G Security discloses a method as claimed in claim 1, but does not disclose sending of at least the challenge or a response in a message in accordance with a Session Initiation Protocol. UMTS security discloses sending the challenge and response in accordance with SIP (pages 202 and 203, Authentication using HTTP Digest AKA). It would have been obvious to one of ordinary skill in the art to modify the method of 3G Security to incorporate SIP of UMTS Security in order to create, modify, and terminate sessions with one or more participants.

Regarding claim 11:

3G Security discloses a method as claimed in claim 1, but does not disclose registering the user equipment with a serving controller of an Internet Multimedia Subsystem. UMTS security discloses registering the UE with a serving controller of an IMS (page 201, Security architecture for the IP multimedia subsystem). It would have been obvious to one of ordinary skill in the art to modify the method of 3G Security to



incorporate IMS of UTMS Security in order to deliver IP multimedia services to end users.

Regarding claims 12 and 13:

3G Security discloses a method as claimed in claim 2, further comprising:  
including in the request for registration a list of security mechanisms supported by the user equipment (page 29 step 1, MS sends sends the UE security capabilities in a list format); concluding at the second controller based on the list that the user equipment supports the second security mechanism instead of the first security mechanism (page 29 step 4, the VLR/SGSN determines which UIAs and UEAs are allowed to be used in order of preference); an indication that the second security mechanism is to be used (page 30 step 5, the VLR/SGSN orders the list as the most preferable occurring at the top of the list); and forwarding the request to the serving controller (page 30 step 5, VLR/SGSN transmits to the SRNC).

3G Security does not disclose the use of including the lists in the headers. It would have been obvious to one of ordinary skill in the art at the time of invention to modify the headers to include the lists of security mechanisms in order to inform the receiver of how to handle the data block.

Regarding claim 14:

3G Security discloses a method as claimed in claim 3, further comprising:  
providing the message comprising a request for a service provided by an application server. It is inherent in an IMS to deliver IP multimedia services to end users, thus a

request for a service provided by an application server would have been obvious to one of ordinary skill in the art at the time of invention.

Regarding claims 15-25:

Claims 15-28 correspond to the method disclosed in the rejection of claims 1-14 and are rejected under the same art and reasoning as claims 1-14.

### ***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

Application/Control Number:  
10/760,521  
Art Unit: 2139

Page 10

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100